DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

January 23, 1995

MEMORANDUM FOR [redacted], DTIC-OCC

SUBJECT: Change 2 to DoD 5200.1-R, dated October 28, 1994

The attached Change 2 to DoD 5200.1-R, "Information Security Program Regulation," June 1986, is provided to DTIC. The DTIC accession number for the basic Regulation and Change 1 is ADA-268022.

For further information, please contact me at (703) 697-4111 or -4112.

Accesion For	
NTIS CRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and / or Special
A-1	

Patricia L. Toppings

PATRICIA L. TOPPINGS
Staff Assistant
Federal Register and
Administrative Section
Directives and Records Branch
Directives and Records Division

DEPARTMENT OF DEFENSE
PUBLICATION SYSTEM TRANSMITTAL

OFFICE OF THE SECRETARY OF DEFENSE
Assistant Secretary of Defense for
Command, Control, Communications, and Intelligence

CHANGE NO. 2
DoD 5200.1-R- CHANGE-2
October 28, 1994
CHANGE 2 to AD-A268022

INFORMATION SECURITY PROGRAM REGULATION

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence has authorized the following changes to DoD 5200.1-R, "Information Security Program Regulation," June 1986:

PAGE CHANGES

Remove: Pages ix through xiv, I-1 through I-4, and V-1 through V-13
Insert: Attached replacement pages and new pages xv, xvi, 1-3a, 1-4a, and Appendices F through I.

PEN CHANGES

Page I-8
Subsection 1-318, lines 2 and 3. Change "Organization" to "Chairman", delete "(OJCS)", and change "and Specified" to "Combatant"

Page I-14
Subparagraph 1-602 a.1.(a)
Line 1. Change "Deputy Under" to "Assistant"
Line 2. Change (Policy) (ODUSD(P))" to "for Command, Control, Communications, and Intelligence (OASD(C3I))"

Delete "including Specified Commands" in the following subparagraphs:
1-602 a.1.(b), lines 2 and 3.
1-602 a.2.(b), lines 2 and 3.

Subparagraph 1-602 a.2.(c). Change "OJCS" to "Chairman of the Joint Chiefs of Staff"

Page III-5, paragraph 3-304 g.
Line 1. Change "ASD(PA)" to "ATSD(PA)"
Line 2. Change "OJCS" to "Chairman of the Joint Chiefs of Staff"

Page IV-10, paragraph 4-304 b., line 18. Change "7920.1" to "8120.1"

Page IV-16, subsection 4-506, line 3. After "Instruction" insert "O-" before "5230.22"

WHEN PRESCRIBED ACTION HAS BEEN TAKEN, THIS TRANSMITTAL SHOULD BE FILED WITH THE BASIC DOCUMENT

NUMBER	DATE	DEPARTMENT OF DEFENSE
5200.1-R, Change 2	October 28, 1994	PUBLICATIONS SYSTEMS TRANSMITTAL

INSTRUCTIONS FOR RECIPIENTS (continued)

Page C-1, Appendix C
After "the" insert "Chairman of the" in the following paragraphs:
1.a., line 4.
2.a., line 1.

Page C-2, Appendix C
After "the" insert "Chairman of the" in the following subparagraphs:
2.a.(1), line 2.
2.b.(4), line 1.

Page C-3, Appendix C
After "the" insert "Chairman of the" in the following subparagraph:
2.b.(5)(b), line 1.

After "the" insert "Chairman of the" in the following subparagraph:
2.c.(3), line 1.

After "the" insert "Chairman of the" in the following subparagraph:
2.c.(4)(b), line 1.

Page C-4, Appendix C
After "the" insert "Chairman of the" in the following paragraph:
4.a, line 1.
4.c, line 1.

EFFECTIVE DATE

The above changes are effective immediately. Forward one copy of revised implementing document to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence within 120 days.

James L. Elmer

JAMES L. ELMER
Director
Correspondence and Directives

Attachments:
37 pages

SD Form 106-2C, MAR 84

Section 6

REMARKING OLD MATERIAL

Chapter V

SAFEKEEPING AND STORAGE

Section 1

STORAGE AND STORAGE EQUIPMENT

Section 2

CUSTODIAL PRECAUTIONS

#First Amendment (Ch 2, 10/28/94)

Section 3

INSTALLATION ENTRY AND EXIT INSPECTION PROGRAM

Chapter VI

COMPROMISE OF CLASSIFIED INFORMATION

CHAPTER VII

ACCESS, DISSEMINATION, AND ACCOUNTABILITY

Section 1

ACCESS

#First Amendment (Ch 2, 10/28/94)

Section 2

DISSEMINATION

Section 3

ACCOUNTABILITY AND CONTROL

CHAPTER VIII

TRANSMISSION

Section 1

METHODS OF TRANSMISSION OR TRANSPORTATION

#First Amendment (Ch 2, 10/28/94)

Section 2

PREPARATION OF MATERIAL FOR TRANSMISSION, SHIPMENT, OR CONVEYANCE

Section 3

RESTRICTIONS, PROCEDURES, AND AUTHORIZATION CONCERNING ESCORT OR HAND-CARRYING OF CLASSIFIED INFORMATION

CHAPTER IX

DISPOSAL AND DESTRUCTION

CHAPTER X

SECURITY EDUCATION

CHAPTER XI

FOREIGN GOVERNMENT INFORMATION

Section 1

CLASSIFICATION

Section 2

DECLASSIFICATION

Section 3

MARKING

#First Amendment (Ch 2, 10/28/94)

Section 4

PROTECTIVE MEASURES

CHAPTER XII

CHAPTER XIII

PROGRAM MANAGEMENT

Section 1

EXECUTIVE BRANCH OVERSIGHT AND POLICY DIRECTION

Section 2

DEPARTMENT OF DEFENSE

#First Amendment (Ch 2, 10/28/94)

Section 3

DOD COMPONENTS

Section 4

INFORMATION REQUIREMENTS

Section 5

DEFENSE INFORMATION SECURITY COMMITTEE

CHAPTER XIV

ADMINISTRATIVE SANCTIONS

APPENDICES

INFORMATION SECURITY PROGRAM REGULATION

CHAPTER 1

GENERAL PROVISIONS

Section 1

REFERENCES

1-100 References

(a) DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982
* (b) Executive Order 12356, "National Security Information," April 2, 1982 *
(c) Information Security Oversight Office (ISOO) Directive No. 1, "National Security Information," June 23, 1982
* (d) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980 *
* (e) DoD 5220.22-R, "Industrial Security Regulation," December 1985 authorized by DoD Directive 5220.2, December 8, 1980 *
* (f) DoD 5220,22-M, "Industrial Security Manual for Safeguarding Classified Information," January 1991, authorized by DoD Directive 5220.22, December 8, 1980 *
* (g) Public Law 83-703, "Atomic Energy Act of August 30, 1954," as amended *
* (h) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 1988 *
* (i) DoD 5200.28-M, "ADP Security Manual," January 1973, authorized by DoD Directive 5200.28, March 21, 1988. *
* (j) Executive Order 12333, "United States Intelligence Activities," December 4, 1981 *
* (k) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13 1988 *
* (l) Patent Secrecy Act of 1952 (35 USC 181-188) *
(m)DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
* (n) DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," March 1986, authorized by DoD Directive 5200.1, June 7, 1982 *
* (o) DoD 0-5200.1-I, "Index of Security Classification Guides," authorized by DoD Directive 5200.1, June 7, 1982[1] *
(p) DoD Directive 5535.2, "Delegations of Authority to the Secretaries of

[1]Published on an annual basis

the Military Departments - Inventions and Patents," October 16, 1980

* (q) DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983
* (r) Independent Offices Appropriations Act (31 U.S.C. 4832)
* (s) DoD Instruction 7230.7, "User Charges," January 29, 1985
* (t) DoD Instruction 8120.1, "Life Cycle Management (LCM) of Automated Information Systems (AIS)," January 14, 1993
* (u) DoD Instruction 0-5230.22, "Controls on the Dissemination of Intelligence Information," July 12, 1988
* (v) National COMSEC Instruction 4005, "Safeguarding and Control of COMSEC Material," October 12, 1979
* (w)National Communications Security Committee (NCSC) Policy Directive 6, April 21, 1990

(x) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," October 6, 1981

(y) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978

(z) DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs," April 21, 1982

* (aa) Joint Army-Navy-Air Force Publications (JANAP) Number 119 and 299

(bb) DoD Directive 5240.6, "Counterintelligence Awareness and Briefing Program," February 26, 1986

* (cc) Executive Order 12065, "National Security Information," June 28, 1978
* (dd) DoD Directive 5210.56, "Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties," February 25, 1992
* (ee) DoD Directive 4140.1, "Material Management Policy," January 4, 1993
* (ff) Joint Chief of Staff memorandum 701-76, Volume II, "Peacetime Reconnaissance and Certain Sensitive Operations, " July 23, 1976
* (gg) DoD Directive 3224.3, "Physical Security Equipment (PSE): Development, Testing Evaluation, Production, Procurement, Deployment, and Support," February 17, 1989

(hh) National COMSEC Instruction 4009, "Protected Distribution Systems," December 30, 1981

* (ii) DoD Directive 5200.12, "Conduct of Classified Meetings," July 27, 1992
* (jj) DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," September 1992
* (kk) DoD Directive 5210.50, "Unauthorized Disclosure of Classified Information," February 27, 1992
* (ll) DoD 5200.2-R, "DoD Personnel Security Program," January 1987 authorized by DoD Directive 5200.2, May 6, 1992

#First Amendment (Ch 2, 10/28/94)

(mm) DoD Directive 5400.4, "Provision of Information to Congress," January 30, 1978

* (nn) DoD Directive 7650.1, "General Accounting Office Access to Records," August 26, 1982

(oo) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

* (pp) National Security Act (50 U.S.C. 403)

* (qq) DoD Directive 4540.1, "Use of Airspace for U.S. Military Aircraft and Firings Over the High Seas," January 13, 1981

* (rr) DoD Directive 5210.41, "Security Policy for Protecting Nuclear Weapons," September 23, 1988

* (ss) DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," December 30, 1992

(tt) Public Law 76-443, "Espionage Act," March 28, 1940

* (uu) Uniform Code of Military Justice (10 U.S.C. 801 et. seq.)

* (vv) Allied Communication Publication (ACP) Number 110

* (ww) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987

* (xx) DoD 5200.1-PH-1, "Classified Information Nondisclosure Agreement (SF 312)," March 1989, authorized by DoD Directive 5200.1, June 7, 1982

* (yy) DoD 5200.1-PH, "Guide to Marking Classified Documents," November 1982, authorized by DoD Directive 5200.1, June 7, 1982

* (zz) DoD Directive C-5230.23, "Intelligence Disclosure Policy (U)," November 18, 1983

* (aaa) DoD Directive 5230.20, "Visits and Assignments of Foreign Representatives," April 24, 1992

* (bbb) DoD TS-5105.21-M-2, "SCI Security Manual - Communications Intelligence Policy (U)," July 1985, authorized by DoD Directive 5105.21, May 19, 1977

* (ccc) DoD C-5105.21-M-1, "SCI Security Manual - Administrative Security (U)," January 1985, authorized by DoD Directive 5105.21, May 19, 1977

(ddd) DoD TS-5105.21-M-3, "SCI Security Manual - TR Policy (U)," November 1985

(eee) National COMSEC Instruction 4003, "Classification Guidelines for COMSEC Information," December 1, 1978

(fff) National COMSEC Instruction 4006, Reporting COMSEC Insecurities," October 20, 1983

(ggg) National Telecommunications and Information Systems Security Instruction 4001, "Controlled Cryptographic Items," March 25, 1985

(hhh) National COMSEC Instruction 4008, "Safeguarding COMSEC Facilities," March 4, 1983

(iii) DoD Directive 5405.2, "Release of Official Information in Litigation and

Testimony by DoD Personnel as Witnesses," July 23, 1985

* (jjj) DoD Directive S-5210.36, "Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the U.S. Government (U) June 10, 1986 *

* (kkk) DoD Directive 0-5205.7, "Special Access Programs (SAP) Policy," January 1989 *

* (lll) MIL-HNBK-1013/1A, "Design Guidelines for Physical Security of Facilities," June 28, 1993 *

Section 2

PURPOSE AND APPLICABILITY

1-200 Purpose

Information of the Department of Defense relating to national security shall be protected against unauthorized disclosure as long as required by national security considerations. This Regulation establishes a system for classification, downgrading, and declassification of information; sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations.

1-201 Applicability

This Regulation governs the DoD Information Security Program and takes precedence over all DoD Component regulations that implement that Program. Under references (a), (b), and (c) it establishes, for the Department of Defense, uniform policies, standards, criteria, and procedures for the security classification, downgrading, declassification, and safeguarding of information that is owned by, produced for or by, or under the control of the Department of Defense or its Components.

1-202 Nongovernment Operations

Except as otherwise provided herein, the provisions of this Regulation that are relevant to operations of nongovernment personnel entrusted with classified information shall be made applicable thereto by contracts or other legally binding instruments. (See DoD Directive 5220.22, DoD 5220.22-R, and DoD 5220.22-M, references (d), (e), and (f).)

1-203 Combat Operations

The provisions of this Regulation relating to accountability, dissemination, transmission, or safeguarding of classified information may be modified by military commanders but only to the extent necessary to meet local conditions in connection with combat or combat-related operations. Classified information should be introduced into forward combat areas or zones or areas of potential hostile activity only when essential to accomplish the military mission.

1-204 Atomic Energy Material

Nothing in this Regulation supersedes any requirement related to "Restricted Data" in the Atomic Energy Act of August 30, 1954, as amended (reference (g)), or the regulations of the Department of Energy under that Act. "Restricted Data" and material designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified to conform with reference (g) and the regulations issued pursuant thereto.

THERE IS NO SUBSTANTIVE INFORMATION ON THIS PAGE.

CHAPTER V

SAFEKEEPING AND STORAGE

Section 1

STORAGE AND STORAGE EQUIPMENT

5-100 General Policy

Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this Regulation represent acceptable security standards. Exceptions to these requirements should be approved by the responsible DoD Component Senior Information Security Authority. This approval authority may be delegated to major commanders. Supplemental or compensatory security measures must be implemented to compensate for the inability to meet the baseline standard. DoD policy concerning the use of force for the protection of classified information is specified in DoD Directive 5210.56 (reference (dd)). Weapons or sensitive items such as funds, jewels, precious metals or drugs shall not be stored in the same container used to safeguard classified information. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence. Current holdings of classified material shall be reduced to the minimum required for mission accomplishment.

5-101 Standards for Storage Equipment

The GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, alarm systems, and associated security devices suitable for the storage and protection of classified information. DoD Directive 3224.3 (reference (gg)) describes acquisition requirements for physical security equipment used within the Department of Defense.

5-102 Storage of Classified Information

Classified information is to be guarded or stored in a locked security container, vault, room, or area, as follows:

a. Top Secret.

Top Secret information shall be stored in the following:

1. A GSA-approved security container or modular vault, in a vault; or in the U.S., in a secure room if under U.S. Government control (see Appendix F). Other rooms that were approved for the storage of Top Secret in the U.S. may continue to be used. When located in

areas not under U. S. Government control, the storage container, vault, or secure room must be protected by an intrusion detection system or guarded when unoccupied. U.S. Government control means access to the classified material is controlled by an appropriately cleared U.S. Government civilian, military, or contractor employee. An intrusion detection system (IDS) used for this purpose shall meet the requirements of Appendix G. Security forces shall respond to the alarmed location within 15 minutes from time of notification.

2. New purchases of combination locks for GSA-approved security containers, vault doors and secure rooms shall conform to Federal Specification FF-L-2740. Existing mechanical combination locks will not be repaired. If they should fail, they will be replaced with locks meeting FF-L-2740.

3. Under field conditions during military operations, the commander may prescribe the measures deemed adequate to meet the storage standard contained in subparagraphs 1. and 2., above.

4. Protection of Top Secret outside the United States requires application of one or more supplementary controls, i.e., continuous guard or duty personnel, inspections of locked containers/vaults or an alarm system.

b. Secret and Confidential

Secret and Confidential information shall be stored in the manner prescribed for Top Secret; or in secure rooms that were approved for the storage of Secret or Confidential material by the DoD Components prior to October 1, 1995. Until October 1, 2002, Secret and Confidential information may also be stored in unapproved or obsolete steel filing cabinets having a built-in combination lock or secured with a lockbar and approved combination padlock in areas under U.S. Government control, or in areas not under U.S. Government control provided the area is protected by an IDS or is guarded when unoccupied. Where IDS is used to protect such information it should meet the requirements of Appendix G, below. Security forces shall respond to the alarmed location within 45 minutes from time of notification.

c. Specialized Security Equipment

1. Military Platforms or Classified Munition Items. The Heads of the DoD Components shall, consistent with this Regulation, delineate the appropriate security measures required to protect classified information stored in containers on military platforms or for classified munition items.

2. Special Purpose Containers. GSA-approved field safes and special purpose one and two drawer light-weight security containers approved by the GSA are used primarily for storage of classified information in the field and in military platforms. Such containers shall be securely fastened to the structure or under constant surveillance to prevent their theft. Use of

these containers in ordinary office environments, or their procurement for this purpose, must be approved by major commands or equivalents.

3. Map and Plan Files. GSA-approved map and plan files are available for storage of odd-sized items such as computer media, maps, charts, and classified equipment.

4. Modular Vaults. GSA-approved modular vaults meeting Federal Specification AA-V-2737 may be used to store classified information as an alternative to vault requirements described in Appendix F.

d. Replacement of Combination Locks. The mission and location of the activity, the classification level and sensitivity of the information, and the overall security posture of the activity determines the priority for replacement of existing combination locks. All system components and supplemental security measures including electronic security systems (e.g., intrusion detection systems, automated entry control subsystems, and video assessment subsystems), and level of operations must be evaluated by the commander when determining the priority for replacement of security equipment. Appendix H, below, provides a matrix illustrating a prioritization scheme for the replacement of existing combination locks on GSA-approved security containers and vault doors. Priority 1 requires immediate replacement.

e. Storage of Bulky Material. Storage areas for bulky material containing classified information may have access openings secured by GSA-approved changeable combination padlocks (Federal Specification FF-P-110 series) or high security key-operated padlocks (Military Specification MIL-P-43607). Other security measures are required, in accordance with paragraph 5-102 a.4. above.

1. The Heads of the DoD Components shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock.

2. Section 1386 of Title 10, United States Code, makes unauthorized possession of keys, key-blanks, keyways or locks adopted by any part of the Department of Defense for use in the protection of conventional arms, ammunition, or explosives, special weapons, and classified equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.

5-103 Procurement of New Storage Equipment

a. New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule. Exceptions may be made by the heads of the DoD Components, with notification to the ASD(C3I). Components should retain and apply serviceable storage equipment made available as consequence of draw downs, contractor turn-in of government furnished equipment, or other events; promptly report excess containers to property disposal; and fulfill

requirements for added equipment through property disposal when that is cost beneficial.

b. Current holdings of classified material shall be reduced to the minimum required for mission accomplishment.

c. Nothing in this Chapter shall be construed to modify existing Federal supply class management assignments made under DoD Directive 5030.47 (reference (ee)).

5-104 Equipment Designations and Combinations

a. Numbering and Designating Storage Facilities. There will be no external mark revealing the level of classified information authorized to be or actually stored in a given container or vault. Priorities for emergency evacuation and destruction will not be marked or posted on the exterior of storage containers or vaults.

b. Combinations to Containers and Vaults

1. Changing: Combinations to security containers, vaults and secure rooms shall be changed only by individuals having that responsibility and an appropriate security clearance. Combinations shall be changed:

(a) When placed in use;

(b) Whenever an individual knowing the combination no longer requires access;

(c) When the combination has been subject to possible compromise;

(d) At least once every two years; or

(e) When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

2. Selecting Combinations. Combinations for each lock shall be unique to that lock and shall have no systematic relationship to other combinations used within a specific office. Combination numbers shall not be derived from numbers otherwise associated with the specific office or its personnel. The number within a combination shall be selected on a random basis without deliberate relationship of one to the other except to provide appropriate variance to operate the lock properly.

3. Classifying Combinations. The combination of a container, vault or secure room used for the storage of classified information shall be assigned a security classification equal to the highest category of the classified information stored therein. Any written record of the

combination shall be marked with the classification. Declassification of combinations occurs at the time they are changed.

4. Recording Storage Facility Data. A record shall be maintained for each vault or secure room door, or container used for storage of classified information, showing location of the door or container, and the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. Standard Form 700, "Security Container Information," shall be used for this purpose.

(a) Part 1 of the SF 700, when completed, shall be placed in an interior location in security cabinets and on vault or secure room doors. To the extent practical, Part 1 shall be on the inside face of the locking drawer of file cabinets, and on the inside surface of map and plan cabinet and vault doors.

(b) SF 700, Parts 2 and 2A, shall be marked conspicuously on their front with the highest level of classification and any special access notice applicable to the information authorized for storage in the container and will be stored in a security container other than the one to which they apply.

(c) Internal security procedures shall provide for prompt notification to the official responsible for the area if a container is found unsecured and unattended or show evidence of unauthorized entry attempt or SF 700 is inaccessible or not available.

(d) Listings of persons having knowledge of the combination shall be continued as necessary on an attachment to Part 2.

5. Dissemination. Access to the combination of a vault or container used for the storage of classified information shall be granted only to those individuals who are authorized access to the classified information to be stored therein.

c. Access Controls. Entrances to secure rooms or areas should be under visual control at all times during duty hours to preclude entry by unauthorized personnel or equipped with electric, mechanical or electromechanical access control devices to limit access during duty hours. Appendix I provides standards for these access control devices; the use of automated systems described therein is encouraged.

5-105 Repair of Damaged Security Containers

Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who have been the subject of a trustworthiness determination in accordance with DoD Regulation 5200.2-R (reference (ll) and are continuously escorted while so engaged.

a. With the exception of frames bent through application of extraordinary stress, a GSA-approved security container manufactured prior to October 1991 (identified by a silver GSA label with black lettering affixed to the exterior of the container) is considered to have been restored to its original state of security integrity as follows:

1. All damaged or altered parts, for example, the locking drawer, drawer head, or lock, are replaced; or

2. Has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, a replacement lock meeting FF-L-2740 is used, and the drilled hole is repaired with a tapered, hardened tool-steel pin, or a steel dowel, drill bit, or bearing with a diameter slightly larger than the hole and of such length that when driven into the hole there shall remain at each end of the rod a shallow recess not less than 1/8 inch nor more than 3/16-inch deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface.

b. In the interests of cost efficiency, the procedures identified in paragraph 5-105.a.2., above, should not be used for GSA-approved security containers purchased after October 1991 (distinguished by a silver GSA label with red lettering affixed to the outside of the container control drawer) until it is first determined whether warranty protection still applies. To make this determination, it will be necessary to contact the manufacturer and provide the serial number and date of manufacture of the container. If the container is under warranty, a lock-out will be neutralized using the procedures described in the Naval Facilities Engineering Service Center (NFESC) Technical Data Sheet (TDS) 2000-SHR (reference (mmm)).

c. Unapproved modification or repair of security containers and vault doors is considered a violation of the container's or door's integrity and the GSA label shall be removed. Thereafter, they may not be used to protect classified information except as otherwise authorized in this Regulation.

5-106 Maintenance and Operating Inspections

a. Maintenance. The Heads of the DoD Components shall establish procedures concerning maintenance of classified material security containers and vaults to accomplish the following:

1. Permit only those persons who have been the subject of a trustworthiness determination in accordance with DoD Regulation 5200.2-R (reference (ll)) to perform maintenance which affects the protective features of the container or vault.

2. Require a record of all maintenance performed on a container or vault be maintained by the using activity and retained with the container or vault. The record shall reflect

the operating problem requiring maintenance, the date maintenance was performed, the name and organization of the maintenance technician, the work accomplished, and the activity official certifying the subsequent proper operation of the container or vault. These records shall be retained for the service life of the container or vault.

3. Refer any discovery of unauthorized tampering or modification of a container or vault to the supporting counterintelligence organization for investigation.

4. Provide a preventive maintenance program for containers and vaults to detect and correct operating problems affecting their security.

b. Operating Inspections. Containers and vaults shall be inspected before being used, and periodically thereafter, and whenever discovered open and unattended or evidence of actual or attempted unauthorized forced or covert entry is present to assure the presence and proper operation of their protective security features before they may continue in use to store classified material.

Section 2

CUSTODIAL PRECAUTIONS

5-200 Responsibilities of Custodians

Anyone who has been duly authorized/appointed to maintain classified information is responsible for its safekeeping, to include storing the material in approved storage containers or facilities when it is not in use or under the supervision of an authorized person.

5-201 Residential Storage Arrangements

Only the Head of a DoD Component, or single designee at the Component headquarters and major command levels, may authorize removal of classified material from designated working areas in off-duty hours, for work at home or otherwise, provided that a GSA-approved security container is furnished and appropriate regulations otherwise provide for the maximum protection possible under the circumstances. Any such arrangements approved before the effective date of this Regulation shall be reevaluated and, if continued approval is warranted, compliance with this paragraph is necessary.

5-202 Care During Working Hours

a. Classified material removed from storage shall be kept under constant surveillance by persons authorized access and having a need to know thereto and, when not in

use, protected from unauthorized view of its classified contents until returned to storage. Such protection shall be provided, as applicable, by the material's unclassified cover or by an appropriate cover sheet. Cover sheets shall be Standard Forms 703, 704, and 705 for, respectively, Top Secret, Secret, and Confidential documents.

b. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, computer and typewriter ribbons, transfer medium and other items containing classified information shall be safeguarded according to the level of classified information they contain and shall be accordingly destroyed after they have served their purpose. Transfer medium include drums, cartridges, belts, sheets, memory, and other material in copiers, printers, facsimile and other devices of items which receive or come in contact with classified information.

c. Destruction of personal computer printer or typewriter ribbons from which classified information can be obtained shall be accomplished in the manner prescribed for classified working papers of the same classification. After the upper and lower sections have been cycled through and overprinted five times in all ribbon or impact or typing positions, fabric ribbons may be treated as unclassified regardless of their previous classified use. Carbon and plastic ribbons and carbon paper that have been used in the production of classified information shall be destroyed in the manner prescribed for working papers of the same classification after initial usage. However, any typewriter ribbon that uses technology which enables the ribbon to be struck several times in the same area before it moves to the next position may be treated as unclassified.

5-203 End-of-Day Security Checks

The Heads of activities that process or store classified information shall establish a system of security checks at the close of each working day to ensure that the area is secure. Standard Form 701, "Activity Security Checklist," shall be used to record such checks. Standard Form 702, "Security Container Check Sheet," shall be used to record the use of all vaults, secure rooms and containers used for the storage of classified material.

5-204 Emergency Planning

a. Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. Such plans shall establish detailed procedures and responsibilities for the protection of classified material to ensure that the material does not come into the possession of unauthorized persons. These plans shall include the treatment of classified information located in foreign countries. Emergency destruction procedures are not needed for activities located inside the 50 states.

b. These emergency planning procedures do not apply to material related to COMSEC. Planning for the emergency protection including emergency destruction under no-notice conditions of classified COMSEC materiel shall be developed in accordance with requirements of NACSI 4006 (reference (fff)).

c. Emergency plans shall provide for the protection of classified material in a manner that will minimize the risk of injury or loss of life to personnel. In the case of fire or natural disaster, the immediate placement of authorized personnel around the affected area, preinstructed and trained to prevent the removal of classified material by unauthorized personnel, is an acceptable means of protecting classified material and reducing casualty risk. Such plans shall provide for emergency destruction to preclude capture of classified material when determined to be required in overseas locations.

5-205 Telecommunications Conversations

a. Classified information shall not be discussed in telephone conversations except over approved secure communications circuits, that is, cryptographically protected circuits or protected distribution systems installed in accordance with National COMSEC Instruction 4009 (reference (hh)).

b. The Secure Telephone Unit-III (STU-III) is approved for classified discussions within the limitations displayed by the STU-III. The need-to-know must be established before discussing classified information.

c. Users of secure telephones shall assure that only persons with appropriate clearance and need-to-know are within hearing range of their conversation.

5-206 Removal of Classified Storage and Information Processing Equipment

All classified storage containers and information processing equipment shall be inspected by properly cleared personnel before removal from protected areas or unauthorized persons are allowed access to them. The inspection shall be accomplished to assure no classified information remains within the equipment. Some examples of equipment which shall be inspected are:

a. Reproduction or facsimile machines and AIS components and other office equipment used to process classified information.

b. GSA-aproved security containers, filing cabinets, or other storage containers used for safeguarding classified information; and

c. Other items of equipment that may inadvertently contain classified information.

5-207 Classified Discussions, Meetings and Conferences

Security requirements and procedures governing disclosure of classified information at conferences, symposia, conventions, and similar meetings, and those governing the sponsorship and attendance of U.S.and foreign personnel at such meetings, are set forth in DoD Directive 5200.12, DoD Instruction 5230.20, DoD 5220.22-R, and DoD 5220.22-M (references (ii), (aa), (e), and (f) respectively.

5-208 Safeguarding of U.S. Classified Information Located in Foreign Countries

Except for classified information that has been authorized for release to a foreign government or international organization pursuant to DoD Directive 5230.11 (reference (oo)), and is under the security control of such government or organization, the retention of U.S. classified material in foreign countries may be authorized only when that material is necessary to satisfy specific U.S. Government requirements. This includes classified material temporarily transferred into a foreign country through U.S. Government personnel authorized to escort or handcarry such material pursuant to Chapter VIII, Section 3, below, as applicable. Whether permanently or temporarily retained, the classified materials shall be stored under U.S. Government control, as follows. See paragraph 5-102 for additional guidance on Top Secret information.

a. At a U.S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

b. At a U.S. Government activity located in a building used exclusively by U.S. Government tenants, if the building is under 24-hour control by U.S. Government personnel.

c. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host-government control, provided the classified material is stored in security containers approved by the GSA and is placed under 24-hour control by U.S. Government personnel.

d. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants, but which is under host-government control, provided the classified material is stored in GSA-approved security containers that are further secured in a locked room or area to which only U.S. personnel have access.

e. When host government and U.S. personnel are collocated, U.S. classified material that has not been authorized for release to the host government under DoD Directive 5230.11 (reference (oo)), shall, be segregated from releasable classified material to facilitate physical control and prevent inadvertent compromise. U.S. classified material that is releasable to the host country need not be subject to the 24-hour U.S. control requirement provided the host

government exercises its own control measures over the pertinent areas or containers during nonduty hours.

f. Foreign nationals shall be escorted while in areas where nonreleasable U.S. classified material is handled or stored. When required by operational necessity, foreign nationals may be permitted, during duty hours, unescorted entry to such areas provided the nonreleasable information is properly stored or is under the direct personal supervision and control of cleared U.S. personnel who can prevent unauthorized access.

g. Under field conditions during military operations, the commander may prescribe the measures deemed adequate to protect classified material.

5-209 Non-COMSEC Classified Information Processing Equipment

The Department of Defense has a variety of non-COMSEC approved equipment to process classified information. This includes copiers, facsimile machines, printers, scanners, cameras, printers for AISs, AISs, electronic typewriters, and other word processing systems among others. Because much of this equipment has known security vulnerabilities, its use can cause unauthorized disclosure.

a. Activities must identify those features, parts, or functions of equipment used to process classified information which may retain all or part of the information. Activity security procedures must prescribe safeguards to:

1. Prevent unauthorized access to that information.

2. Replace and destroy equipment parts as classified material when the information cannot be removed from them. Alternatively, the equipment may be designated as "classified" and protected at least at the retained information's classification level.

b. Activities will select equipment that performs the needed function and presents the lowest acceptable risk to the classified information the equipment processes.

c. Activities will comply with guidance on security vulnerabilities issued by appropriate authority and must report equipment problems and failures.

5-210 Reporting Equipment Problems and Vulnerabilities

a. The equipment that the Department of Defense uses to safeguard, destroy or process classified information can fail to function properly or otherwise perform in a way that threatens that information. When that occurs, responsible individuals within the using activities must promptly:

1. Restore the protection to the information.

2. Report the incident to their Component security office. Such reports shall:

(a) Be classified or transmitted by secure means, as warranted by the nature of the problem.

(b) Describe the problem; the equipment's type, manufacturer, and any serial number; the number of equipment units involved; and any means found to overcome the problem.

(c) Be in addition to those made to logistics, supply, or contracting offices, or those made in reporting security violations.

b. Component security offices receiving such reports shall assess the impact on other Component activities and advise them accordingly. They shall also promptly send a copy of the initial and any subsequent reports to the Director, Counterintelligence and Security Programs, ODASD(I&S), OASD(C3I). They shall include their assessment of the impact and a summary of the related Component actions.

c. Problems or vulnerabilities with COMSEC equipment and Controlled Cryptographic Items shall be reported as prescribed by the controlling COMSEC authorities rather than under this subsection. The COMSEC authority shall promptly coordinate these reports and correcting actions with the Director, Counterintelligence and Security Programs, OASD(C3I), when the problems or vulnerabilities are common to all such equipment.

Section 3

INSTALLATION ENTRY AND EXIT INSPECTION PROGRAM

5-300 Policy

Commanders shall prescribe procedures for inspecting persons, their property and vehicles at entry and exit points of installations or at designated secure areas within an installation and for search of persons and their possessions while on an installation.

a. This shall include determination of whether inspections are randomly conducted or mandatory for all, and shall prescribe procedures to ensure the safeguarding of classified information.

b. Examinations of individuals and their possessions while on the installation for the primary purpose of obtaining evidence is classified as a "search" under the fourth amendment and separate guidance regarding the conduct of these searches shall be issued.

c. All procedures shall be reviewed for legal sufficiency by the general counsel or legal advisor before issuance. These procedures shall require Commanders to consult with their servicing Judge Advocate or other legal advisor before authorizing gate inspections.

#First Amendment (Ch 2, 10/28/94)

APPENDIX F

VAULT AND SECURE ROOM CONSTRUCTION STANDARDS

1. Vault

a. Floor and Walls. Eight inches of concrete reinforced to meet current structural standards. Walls are to extend to the underside of the roof slab above.

b. Roof. Monolithic reinforced-concrete slab of thickness to be determined by structural requirements, but not less than the floors and walls.

c. Ceiling. The roof or ceiling must be reinforced concrete of a thickness to be determined by structural requirements, but not less than the floors and walls.

d. Vault door and frame unit should conform to Federal Specification AA-D-2757 Class 8 vault door, or Federal Specification AA-D-600 Class 5 vault door.

2. Secure Room

a. The walls, floor, and roof construction of secure rooms must be of permanent construction materials; i.e., plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling and attached with permanent construction materials, wire mesh or 18 gauge expanded steel screen.

b. Ceiling. The ceilings shall be constructed of plaster, gypsum, wallboard material, hardwood, or any other acceptable material.

c. Doors. The access door to the room shall be substantially constructed of wood or metal. The hinge pins of outswing doors shall be peened, brazed, or spot welded to prevent removal. Door should be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740.

d. Windows. Windows which are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, shall be constructed from or covered with materials which will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

e. Openings. Utility openings such as ducts and vents should be kept at less than man-passable (96 square inches) opening. Openings larger than 96 square inches will be hardened in accordance with Military Handbook 1013/1A (reference (lll)).

APPENDIX G

IDS STANDARDS

1. An IDS must detect an unauthorized penetration in the secured area. An IDS complements other physical security measures and consists of the following:

a. Intrusion Detection Equipment (IDE).

b. Security forces.

c. Operating procedures.

2. System Functions

a. IDS components operate as a system with the following four distinct phases:

(1) Detection.

(2) Communications.

(3) Assessment.

(4) Response.

b. These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.

(1) Detection: The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area to the Premise Control Unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise a "zone" at the monitor station. This shall be used as the definition of an alarmed zone for purposes of this Regulation.

(2) Reporting: The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. Another signal is added to the communication for supervision to prevent compromise of the communication scheme. This supervised signal is intended to disguise the information and protect the IDS against tampering or injection of false information by an intruder. The supervised signal is sent by the PCU through the transmission link to the monitor station. Inside the monitor station either a dedicated panel or central processor monitors information from the PCU signals.

When an alarms occur, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

(3) Assessment: The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force.

(4) Response: The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response phase must also determine the precise nature of the alarm and take all measures necessary to safeguard the secure area.

3.

a. As determined by the commander all areas that reasonably afford access to the container, or where classified data is stored should be protected by IDS unless continually occupied. Prior to the installation of an IDS, commanders shall consider the threat, vulnerabilities, in-depth security measures and shall perform a risk analysis.

b. Acceptability of Equipment: All IDE must be UL-listed (or equivalent) and approved by the DoD Component or government contractor. Government installed, maintained, or furnished systems are acceptable.

4.

a. Transmission Line Security: When the transmission line leaves the facility and traverses an uncontrolled area, Class I or Class II line supervision shall be used.

(1) Class I: Class I line security is the achieved through the use of DES or an algorithm based on the cypher feedback or cypher block chaining mode of encryption. Certification by NIST or another independent testing laboratory is required.

(2) Class II: Class II line supervision refers to systems in which the transmission is based on pseudo random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum 6 month period. Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

b. Internal Cabling: The cabling between the sensors and the PCU should be dedicated to IDE and must comply with national and local code standards.

c. Entry Control Systems: If an entry control system is integrated into an IDS, reports from the automated entry control system should be subordinate in priority to reports from intrusion

alarms.

d. Maintenance Mode: When an alarm zone is placed in the maintenance mode, this condition shall be signaled automatically to the monitor station. This signal must appear as an alarm or maintenance message at the monitor station and the IDS shall not be securable while in the maintenance mode. The alarm or message must be continually visible at the monitor station throughout the period of maintenance. A standard operating procedure must be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods shall be archived in the system. A self-test feature shall be limited to one second per occurrence.

e. Annunciation of Shunting or Masking Condition: Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

f. Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the secure area.

g. Power Supplies: Primary power for all IDE shall be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment shall change power sources without causing an alarm indication.

(1) Emergency Power: Emergency power shall consist of a protected independent backup power source that provides a minimum of 4 hours operating power battery and/or generator power. When batteries are used for emergency power, they shall be maintained at full charge by automatic charging circuits. The manufacturer's periodic maintenance schedule shall be followed and results documented.

(2) Power Source and Failure Indication: An illuminated indication shall exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station shall indicate a failure in power source, a change in power source, and the location of the failure or change.

h. Component Tamper Protection: IDE components located inside or outside the secure area should be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection should be provided.

5. System Requirements

a. Independent Equipment. When many alarmed areas are protected by one monitor station, secure room zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

b. Access and/or Secure Switch and PCU: No capability should exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs must be located inside the secure area and should be located near the entrance. Assigned personnel should initiate all changes in access and secure status. Operation of the PCU may be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

c. Motion Detection Protection: Secure areas that reasonably afford access to the container or where classified data is stored should be protected with motion detection sensors; e.g., ultrasonic and passive infrared. Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector shall cause an immediate and continuous alarm condition.

d. Protection of Perimeter Doors: Each perimeter door shall be protected by a balanced magnetic switch (BMS) that meets the standards of UL 634.

e. Windows: All readily accessible windows (within 18 feet of ground level) shall be protected by an IDS, either independently or by the motion detection sensors in the space.

f. IDS Requirements for Continuous Operations Facilities: A continuous operations facility may not require an IDS. This type of secure area should be equipped with an alerting system if the occupants cannot observe all potential entrances into the room. Duress devices may also be required.

g. False and/or Nuisance Alarm: Any alarm signal transmitted in the absence of detected intrusion or identified as a nuisance alarm is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. All alarms shall be investigated and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms should not exceed 1 in a period of 30 days per zone.

6.

a. IDS Installation and Maintenance Personnel: Alarm installation and maintenance should be accomplished by U.S. citizens who have been subjected to a trustworthiness determination in accordance with DoD Regulation 5200.2-R (reference (ll).

b. Monitor Station Staffing: The monitor station should be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination in accordance with DoD Regulation 5200.2-R (reference (ll).

Appendix H

PRIORITY FOR REPLACEMENT

Priorities range from 1 to 4, with 1 being the highest and 4 the lowest.

LOCK REPLACEMENT PRIORITIES IN THE UNITED STATES AND ITS TERRITORIES

ITEM	TS/SAP	TS	S/SAP	S-C
Vault Doors	1	1	3	4
Containers (A)*	3	4	4	4
Containers (B)**	1	1	1	2
Crypto	1	1	2	2

LOCK REPLACEMENT PRIORITIES OUTSIDE THE UNITED STATES AND ITS TERRITORIES

ITEM	TS/SAP	TS	S/SAP	S-C
Vault Doors	1	1	2	2
Containers (A)*	2	2	3	3
Containers (B)**	1	1	1	2
Crypto	1	1	2	2
High Risk Areas	1	1	1	1

* A - Located in a controlled ennvironment where the Department of Defense has the authority to prevent unauthorized disclosure of classified information. The Government may control or deny access to the space, post guards, require identification, challenge presence, innspect packages, program elevators, or take other reasonable measures necessary to deny unauthorized access.

**B - Located in an uncontrolled area without perimeter security measures.

APPENDIX I

ACCESS CONTROLS

1. Access Controls:

The perimeter entrance should be under visual control at all times during working hours to preclude entry by unauthorized personnel. This may be accomplished by several methods (e.g., employee work station, guard, CCTV). Regardless of the method used, an access control system shall be used on the entrance. Uncleared persons are to be escorted within the facility by a cleared person who is familiar with the security procedures at the facility.

a. Automated Entry Control Systems: An automated entry control system may be used to control admittance during working hours instead of visual control, if it meets the AECS criteria stated below.

The automated entry control system must identify an individual and authenticate the person's authority to enter the area through the use of an identification (ID) badge or card.

(1) ID Badges or Key Cards. The ID badge or key card must use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) Personal Identity Verification. Personal identity verification (Biometrics Devices) identifies the individual requesting access by some unique personal characteristic, such as:

(a) Fingerprinting

(b) Hand Geometry

(c) Handwriting

(d) Retina scans

(e) Voice recognition.

A biometrics device may be required for access to the most sensitive information.

2. In conjunction with subparagraph 1.a.(1), above, a personal identification number (PIN) may be required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

3. Authentication of the individual's authorization to enter the area must be accomplished within the system by inputs from the ID badge/card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than the required access level.

4. Protection must be established and maintained for all devices or equipment which constitute the entry control system. the level of protection may vary depending upon the type of device or equipment being protected.

a. Location where authorization data and personal identification or verification data is input, stored, or recorded must be protected.

b. Card readers, keypads, communication or interface devices located outside the entrance to a controlled area shall have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.

c. Keypad devices shall be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

d. Systems that use transmission lines to carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area shall have line supervision.

e. Electric strikes used in access control systems shall be heavy duty, industrial grade.

5. Access to records and information concerning encoded ID data and PINs shall be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system shall be limited to the fewest number of personnel as possible. Such data or software shall be kept secure when unattended.

6. Records shall be maintained reflecting active assignment of ID badge/card, PIN, level of access, and similar system-related records. Records concerning personnel removed from the system shall be retained for 90 days. Records of entries shall be retained for at least 90 days or until investigations of system violations and incidents have been investigated, resolved and recorded.

7. Personnel entering or leaving an area shall be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirmation of need to know and access. The Heads of DoD Components may approve the use

of standardized AECS which meet the following criteria:

a. For a Level 1 key card system, the AECS must provide a .95 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.05 probability after three attempts to gain entry.

b. For a Level 2 key card and PIN system, the AECS must provide a 0.97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.010 probability after three attempts to gain entry have been made.

c. For a Level 3 key card and PIN and biometrics identifier system, the AECS must provide a 0.97 probability of granting access to an unauthorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.005 probability after three attempts to gain entry have been made.

8. Electric, Mechanical, or Electromechanical Access Control Devices. Electric, mechanical, or electromechanical devices which meet the criteria stated below may be used to control admittance to secure areas during duty hours if the entrance is under visual control. These devices are also acceptable to control access to compartmented areas within a secure area. Access control devices must be installed in the following manner:

a. The electronic control panel containing the mechanical mechanism by which the combination is set is to be located inside the area. The control panel (located within the area) will require only minimal degree of physical security designed to preclude unauthorized access to the mechanism.

b. The control panel shall be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.

c. The selection and setting of the combination shall be accomplished by an individual cleared at the same level as the highest classified information controlled within.

d. Electrical components, wiring included, or mechanical links (cables, rods and so on) should be accessible only from inside the area, or, if they traverse an uncontrolled area, they should be secured within protecting covering to preclude surreptitious manipulation of components.